

MICHIGAN STATE

UNIVERSITY

Beta Presentation

Enhanced MISP User Interface

The Capstone Experience

Team GM

Jordyn Rosario

Alex Richards

Marven Nadhum

Jake Rizkallah

Noah Anderson

Department of Computer Science and Engineering
Michigan State University

Fall 2021



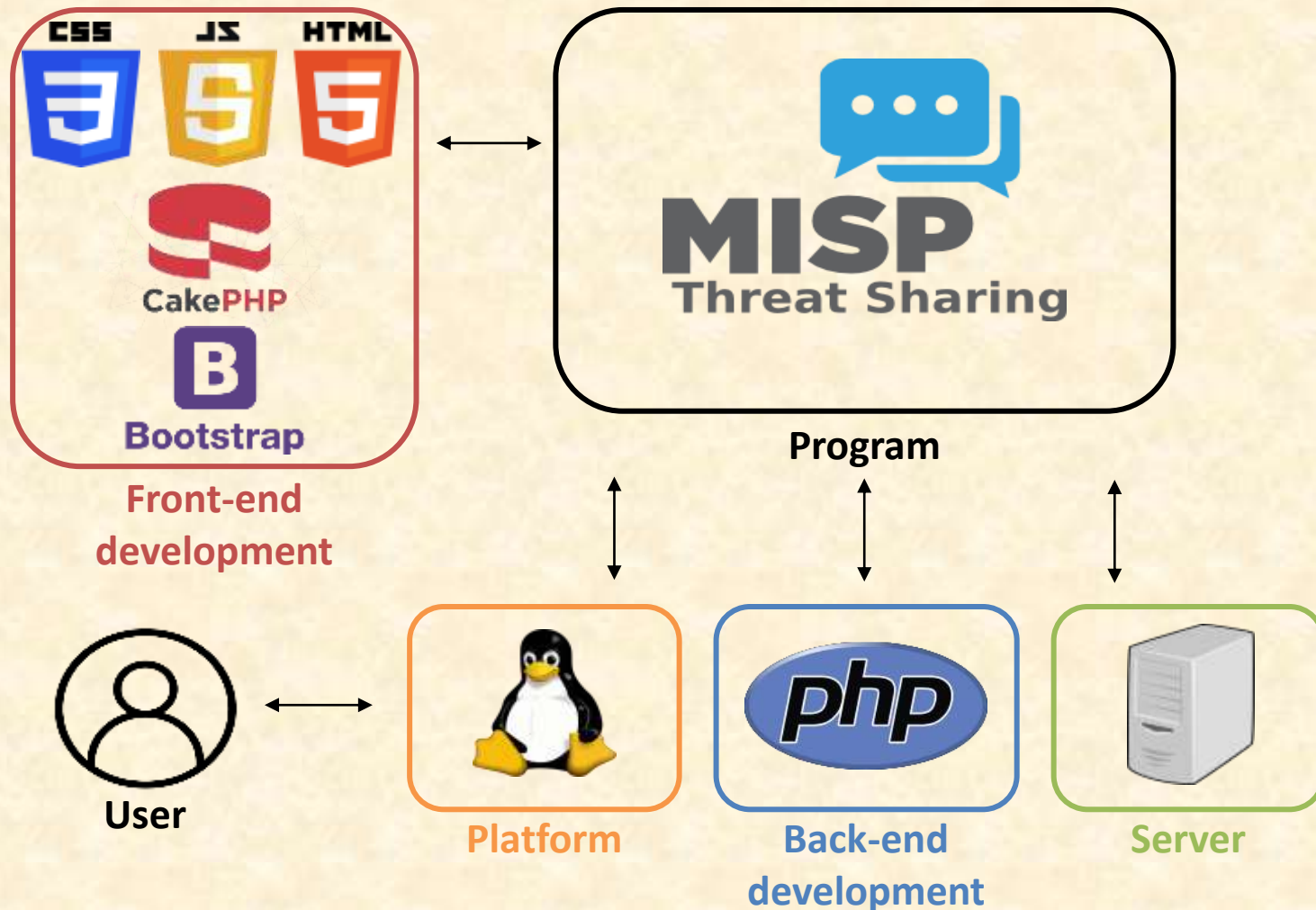
*From Students...
...to Professionals*

Project Overview

- MISP, Malware Information Sharing Platform, is an open-source software that allows for threat intelligence to be share with security analysts
- Enhance UI to allow for customization of components and a simpler feel that provides a straightforward experience
- Improve existing functionalities to provide ease of use and increase productivity for GM's security analysts



System Architecture



Events

The screenshot displays the MISP (Malware Information Sharing Platform) Events page. The interface includes a navigation menu on the left with options like 'List Events', 'Add Event', and 'REST client'. The main content area shows a table of events with columns for 'Published', 'Creator org', 'Owner org', 'ID', 'Tags', 'Creator user', 'Date', 'Info', 'Distribution', and 'Actions'. The table lists various security events, such as 'ICS-CERT.io', 'Malware Analysis Report (AR19-100A)', and 'OSINT - Maria botnet'. Each event entry includes a list of tags and a 'Favorite' button. The browser's address bar shows 'https://localhost/events/index'.

| Published | Creator org | Owner org | ID | Tags | Creator user | Date | Info | Distribution | Actions |
|-------------------------------------|-------------|-----------|--------|---|------------------|------------|--|----------------|---------|
| <input checked="" type="checkbox"/> | ICS-CERT.io | ORGNAME | 7 352 | tip:white, #the-ics-sectors-DHS-critical-sectors-transport, Favorite | admin@admin.test | 2021-09-25 | MeteorExpress Mysterious Wiper Paralyzes Iranian Trains with Epic Troll | All < | |
| <input checked="" type="checkbox"/> | | ORGNAME | 7 1401 | tip:white, type:OSINT, asint:lifetime=perpetual, asint:certainty=50, misp-galaxy:mitre-enterprise-attack-intrusion-set=Lazarus Group, misp-galaxy:mitre-intrusion-set=Lazarus Group, misp-galaxy:threat-actor=COVELLITE, Favorite | admin@admin.test | 2019-04-03 | Malware Analysis Report (AR19-100A) MAR-10135538-8 4C North Korean 'Bojars' HOPLIGHT MAR-10135536.r6.v1 | All < | |
| <input checked="" type="checkbox"/> | | ORGNAME | 7 1542 | type:OSINT, asint:lifetime=perpetual, asint:certainty=50, tip:white, Favorite | admin@admin.test | 2021-09-17 | OSINT - Maria botnet | All < | |
| <input checked="" type="checkbox"/> | ORGNAME | ORGNAME | 7 1568 | asint:source-type=block-or-filter-list, Favorite | admin@admin.test | 2021-10-15 | ci-badguys.txt feed | Organisation < | |
| <input checked="" type="checkbox"/> | ORGNAME | ORGNAME | 7 1567 | asint:source-type=block-or-filter-list | admin@admin.test | 2021-10-15 | cybercrime-tracker.net - all feed | Organisation < | |
| <input checked="" type="checkbox"/> | ORGNAME | ORGNAME | 7 84 | asint:source-type=block-or-filter-list | admin@admin.test | 2021-10-06 | blockrules of rules.emergingthreats.net feed | Organisation < | |
| <input checked="" type="checkbox"/> | EUDES0 | ORGNAME | 7 1570 | circ:incident-classification=malware, circ:incident-classification=phishing, tip:white | admin@admin.test | 2021-10-27 | SQUIRRELWAFFLE Leverages matpam to deliver Dabbot, Cobalt Strike | All < | |
| <input checked="" type="checkbox"/> | | ORGNAME | 7 1385 | type:OSINT, asint:lifetime=perpetual, asint:certainty=50, tip:white | admin@admin.test | 2021-10-24 | Malware Discovered in Popular RPM Package, us-parser-ii | All < | |
| <input checked="" type="checkbox"/> | ORGNAME | ORGNAME | 7 411 | asint:source-type=block-or-filter-list | admin@admin.test | 2021-10-06 | Phishrank online valid phishing feed | Organisation < | |
| <input checked="" type="checkbox"/> | ORGNAME | ORGNAME | 7 1564 | | admin@admin.test | 2021-10-13 | perpetual | Organisation < | |
| <input checked="" type="checkbox"/> | EUDES0 | ORGNAME | 7 1565 | tip:white | admin@admin.test | 2021-10-08 | FemOnLake: Previously unknown malware family targeting Linux | All < | |
| <input checked="" type="checkbox"/> | EUDES0 | ORGNAME | 7 234 | tip:white | admin@admin.test | 2021-09-14 | Operation 'Harvost': A Deep Dive into a Long-term Campaign | All < | |
| <input checked="" type="checkbox"/> | EUDES0 | ORGNAME | 7 538 | tip:white | admin@admin.test | 2021-10-02 | A wolf in sheep's clothing: Actors spread malware by leveraging trust in Amnesty International and fear of Pegasus | All < | |



Event Attributes

| Date | Org | Category | Type | Value | Tags | Galaxies | Comment | Correlate | Related Events | Feed hits | IDS | Distribution | Sightings | Activity | Actions |
|------------|-----|-------------------|---------|---|------|----------|----------------------------|-----------|----------------|-----------|-----|--------------|-----------|----------|---------|
| 2021-09-01 | | External analysis | link | https://citizenlab.ca/2021/08/bahrain-hackers-activists-with-mo-group-zero-click-phishing-exploit/ | | | | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Network activity | domain | m6nq23feval.info | | | Websites linked to Pegasus | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Network activity | domain | siyasmehbus.com | | | Websites linked to Pegasus | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Network activity | domain | breakingnewyork.info | | | Websites linked to Pegasus | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Network activity | domain | i-election-online.com | | | Websites linked to Pegasus | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Network activity | domain | washington-today.com | | | Websites linked to Pegasus | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Network activity | domain | human-rights-news.com | | | Websites linked to Pegasus | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Network activity | ip-dst | 92.222.71.344 | | | | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Network activity | domain | helpusfind.biz | | | New Pegasus infrastructure | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Network activity | domain | news-now.co | | | New Pegasus infrastructure | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Network activity | domain | reunionlove.net | | | New Pegasus infrastructure | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Network activity | domain | visibileminder.net | | | | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Network activity | domain | youneedajelly.net | | | | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Network activity | ip-dst | 208.250.217.55 | | | | | | 2 | | Inherit | (0/0/0) | | |
| 2021-09-01 | | Other | comment | Working hard to create a new website design. Stay in touch! | | | Maintenance decoy | | | | | Inherit | (0/0/0) | | |



Public Save Search Query

The screenshot shows the MISP web interface. The top navigation bar includes links for Home, View Saved Searches, Add Search Query, and a search input field. The main content area is titled "Saved Searches" and displays a table of saved search queries. The table has columns for ID, User, Title, Value, Created at, and Actions. There are 6 records shown, with the first 5 visible on this page. The footer contains a download link and a version notice.

| ID | User | Title | Value | Created at | Actions |
|----|------------------|--|---|---------------------|-----------------|
| 12 | admin@admin.test | Rookkits | https://localhost/events/index/searchtag-240 | 2021-11-14 17:35:59 | [edit] [delete] |
| 11 | admin@admin.test | Spyware | https://localhost/events/index/searchtag-226 | 2021-11-14 17:34:58 | [edit] [delete] |
| 10 | admin@admin.test | Ransomware | https://localhost/events/index/searchtag-1026 | 2021-11-14 17:34:29 | [edit] [delete] |
| 9 | admin@admin.test | High level threat open source intelligence | https://localhost/events/index/searchtag-28/searchtaglevel-1 | 2021-11-14 17:34:06 | [edit] [delete] |
| 8 | admin@admin.test | October 2021 events | https://localhost/events/index/searchDatefrom:2021-08-01/searchDateuntil:2021-10-31 | 2021-11-14 17:31:20 | [edit] [delete] |

Page 1 of 2, showing 5 records out of 6 total, starting on record 1, ending on 5

Download: MISP public key | This is an initial install Powered by MISP 2.4.250 Please configure and harden accordingly - 2021-11-14 17:52:11



Private Save Search Query

The screenshot displays the MISP web interface for PrivateSaveSearch. The browser address bar shows the URL `https://localhost/PrivateSaveSearch`. The navigation menu includes: MISP, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, and API. The main content area is titled "Your Saved Searches" and features a table of saved queries. The table has columns for ID, User, Title, Value, Created at, and Actions. Three queries are listed, all created on 2021-11-14 17:37:11. A search bar with the placeholder "Enter value to search" and a "Filter" button is located to the right of the table. The footer contains the text: "Download: PGP public key" and "This is an initial install. Powered by MISP 2.8.151. Please configure and harden accordingly - 2021-11-14 17:51:37".

| ID | User | Title | Value | Created at | Actions |
|----|------------------|----------------------------------|--|---------------------|---------|
| 7 | admin@admin.test | targeted systems (Windows) | <code>https://localhost/events/index/searchtag:577</code> | 2021-11-14 17:37:11 | |
| 6 | admin@admin.test | ms-care-malware (linux) - Botnet | <code>https://localhost/events/index/searchtag:242,searchall:botnet</code> | 2021-11-14 17:37:11 | |
| 5 | admin@admin.test | ms-care-malware (linux) | <code>https://localhost/events/index/searchtag:170</code> | 2021-11-14 17:37:11 | |



What's left to do?

- Ensure UI consistency across platform
- Test for and fix possible bugs
- Cleaning up code
- Get code into deliverable format



Questions?

?

?

?

?

?

?

?

?

?

